AVOIDING IDENTITY THEFT
IN THE AGE OF INFORMATION COMPROMISE

prevention tips to share with your friends and family

AM I A VICTIM OF IDENTITY THEFT?

Many of us have gotten notice saying our personal information has been exposed. Whether your information was lost, stolen or exposed, it doesn't make you an identity theft victim. A criminal has to use your information for you to be a victim of identity theft. This difference is important because the road map for resolving identity theft is different than the one for avoiding it.

WHY DO I NEED TO DO ANYTHING?

There are several tools you can use to prevent identity theft. You are the best line of defense. While credit report monitoring services can be helpful, they can't catch everything. Being aware can save you lots of time and effort if someone does use your information.

ACTION STEPS

Consider a security freeze. A security freeze is FREE and stops anyone from looking at your credit report. It stops criminals from opening up new accounts using your information. The freeze does not affect your existing accounts, so you will need to monitor those carefully.

- You must contact EACH credit reporting agency to place the freeze. If you have trouble placing the freeze online, try placing it by phone.
- Remember, you will need to temporarily or permanently lift it using your PINs before applying for a good or service that requires a credit check. Keep your PINs private and in a safe place.
- It is FREE to place and lift the freeze.

Call all three to place the Freeze.
Call one to place the Fraud Alert.

Equifax: 800-685-1111
TransUnion: 800-680-7289
Experian: 888-397-3742

THE FRAUD ALERT AND SECURITY FREEZE ARE FREE!

Check your credit reports. Request your free annual credit report from each of the three major credit reporting agencies at www.annualcreditreport.com or by calling 877-322-8228. Go over the reports carefully, marking any information that doesn't belong to you.

Place a fraud alert. A fraud alert can make it harder for an identity thief to open accounts in your name. When you have an alert on your report, a business must take extra steps to verify it is you applying for the good or service. It also allows you to get a free report from each credit reporting agency.

Monitor your statements. Make sure your financial and benefits statements are coming in on time and are correct.

ID THEFT CLUES

IDENTITY THIEVES CAN USE YOUR INFORMATION ANY WAY YOU DO

Once identity thieves have your personal information, they can drain your bank account, run up charges on your credit cards, open new utility accounts, or get medical treatment using your health insurance. An identity thief can even file a tax return in your name. In some extreme cases, a thief might even give your name to the police during an arrest.

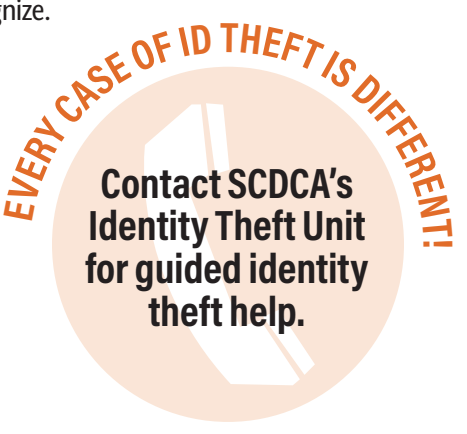
SIGNS YOU MIGHT BE A VICTIM OF IDENTITY THEFT

Financial Accounts

- You see withdrawals from your bank account that you can't explain.
- You don't get your bills or other mail or get a bill for something you don't recognize.
- Debt collectors call you about debts that aren't yours.
- You find unfamiliar addresses, accounts or charges on your credit report.

Other Clues

- Medical providers bill you for services you didn't use.
- Your health plan rejects your legitimate medical claim because the records show you've reached your benefits limit.
- The IRS notifies you that more than one tax return was filed in your name, or that you have income from an employer you don't work for.
- You find errors on your social security statement.



THINKING OUTSIDE THE BOX

Consider these other tools for protecting your accounts. Many banks offer text or email account alerts that may fit your needs.

- Get a notice if your balance falls below a certain number.
- Get a notice if a charge greater than $X (i.e. $100) hits your account.

These alerts can make watching existing accounts less of a hassle.

Online account safety. Update your online account information often, using strong passwords. Don't share your passwords or use the same ones for all your accounts. Consider using multi-factor authentication, if it's offered. It adds an extra step (like a text message code or finger print) to your login process, making it more secure.

WATCH OUT FOR SCAMS

Scam artists follow the headlines. Imposter scammers could have more information about you than ever, making their phone calls, emails and other communications seem even more convincing. When fielding unsolicited communications of any type, know the red flags of a scam. Find more information by visiting www.consumer.sc.gov and clicking REPORT IDENTITY THEFT.

South Carolina Department of Consumer Affairs
2221 Devine St. STE 200 • PO Box 5757 • Columbia, SC 29250
800-922-1594 • www.consumer.sc.gov